STAFF REPORT

DATE: July 10, 2018

TO: City Council

FROM: Darren Pytel, Police Chief

SUBJECT: Surveillance Technology – GeoTime

Recommendation

Informational. The Davis 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 the use of GeoTime technology. 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:

GeoTime uses call and text data obtained from search warrants to produce 3 dimensional maps. The maps are generally used to show movement of phones over time (hours, days, etc.) which can aid in the investigation of a criminal case. In addition to call and text data, GeoTime can also import data from the following sources: GPS, Cellebrite, XRY, Twitter, Facebook, Snapchat and Instagram. With the data plotted onto a map, GeoTime can then produce supplementary analytical products such as charts, timelines, and animated videos/PPTs for courtroom presentation purposes such as at preliminary hearings and trials.

(b) If applicable, the location(s) it may be deployed and crime statistics for any location(s);
This technology is not deployed. Cell phones are constantly used/carried by those involved in crime and oftentimes have critical information used in investigations/prosecutions. Data can also be used to exonerate individuals believed to be involved in crime.

(c) An assessment identifying any potential impact on civil liberties and civil rights and discussing any plans to safeguard the rights of the public;
The data obtained to use the technology is gathered pursuant to search warrant for criminal cases. The data is maintained as a police record and is confidential and discovered properly for criminal cases. The technology does electronically plot out data derived from cellphones and can be used to track the locations of where a person was.

(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
$3,975.00 (already purchased)

Personnel Costs
No additional costs. Saves significant staff time having program do the plotting rather than a staff having to hand plot information.

Ongoing Costs
$924/year maintenance fee

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;
No.

(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.
None noted. This is commonly used software for use in criminal investigations.

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.

This technology is specifically intended to assist in the investigation of cases by collating and displaying raw phone call and text detail records on a map and into other analytical products such as: charts, PPTs, videos, and timelines.

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

This technology may only be used upon request by a sworn officer to advance or assist in the investigation of a criminal case. Employees assigned to Investigations or Crime Analysis AND who have also received official GeoTime training may use the technology.

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

GeoTime does not independently collect data; however, GeoTime is compatible with open source data using metadata on many different types of open source files.

(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.

Products made using GeoTime (maps, PPTs, timelines, etc.) may only be used or accessed by the requesting party. If the product has evidentiary value and is therefore included as a supplement to a criminal case in our RMS, the product may be discoverable.

(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.

Products made using GeoTime are generally kept in digital format and are password protected. If a requestor prints materials produced from GeoTime, the requestor is responsible for keeping said materials in a locked location when not in use to prevent unauthorized access.

(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.

Materials produced from GeoTime will be kept as long as necessary and that time period is case specific. At the conclusion of an investigation, should the requestor no longer need the materials, the requestor should shred physical copies and delete any digital copies.

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

This is confidential investigation information. When used for criminal prosecution is available to the prosecutor and defense.

(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.
N/A

(i) Training: The training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology.
Access to information produced by GeoTime is restricted to sworn officers, attorneys and those assigned to Crime Analysis. Employees assigned to Investigations or Crime Analysis AND who have also received official GeoTime training may use the 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.
The Police Services Manager is responsible for overseeing and auditing the use of the technology and to ensure this policy is followed.