Surveillance Use Policy

(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 criminal investigations 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 department member. 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 will 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 and exempt from public disclosure when used for criminal prosecutions. It is available to the prosecutor and defense through the discovery process which is governed by state and federal law and overseen by the courts.

Crime maps are public information and are shared via the web, media, social media and other public forums.

(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.
Extracted data that is not public information is generally only used by the Davis Police Department. Extracted data may be shared with other law enforcement agencies who are involved in a joint criminal investigation, or who are conducting their own criminal investigation. Sharing data requires authorization from command staff. Data can also be shared with various prosecutors’ offices, including District Attorney’s, State Attorney or United States Attorney, as well as with criminal defendants and their attorneys through the criminal discovery process or as otherwise required by law.

(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 Support Services Manager is responsible for overseeing and auditing the use of the technology and to ensure this policy is followed.

The use of the technology is documented in a criminal police report. A member is 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 technology. The review should include an analysis of the cost, benefit and effectiveness of the technology, 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 and other applicable advisory bodies. Any recommendations for training or policy will be promptly addressed.

Darren Pytel
Police Chief
October 30, 2018