Surveillance Use Policy for StarChase GPS Vehicle Tracking Technology

In accordance with Palo Alto Municipal Code Section PAMC 2.30.680(d), the Surveillance Use Policy for the Police Department's use of StarChase GPS Vehicle Tracking technology is as follows:

1. **Intended Purpose.** The technology is used by the Palo Alto Police Department to remotely affix a GPS tracking device to a wanted vehicle, which is being pursued or is about to be pursued, for the purpose of remotely tracking the vehicle's movements and apprehending it later. This procedure provides officers with a potential alternative to engaging in, or continuing, a vehicle pursuit.

2. **Authorized Uses.** Department personnel may only access and use the StarChase system for official and legitimate law enforcement purposes consistent with this Policy.

   The following uses of the StarChase system are specifically prohibited:
   a. Harassment or Intimidation: It is a violation of this Policy to use the system to harass and/or intimidate any individual or group.
   b. Personal Use: It is a violation of this Policy to use the system or data for any personal purpose.
   c. First Amendment Rights. It is a violation of this policy to use the system or associated data for the purpose or known effect of infringing upon First Amendment rights of any person.
   d. Invasion of Privacy: Except when done pursuant to a court order such as a search warrant or pursuant to specific exceptions (explained below), it is a violation of this Policy to utilize the system to record the geographic location of vehicles not exposed to public view (e.g., vehicles on a public road or street, or that are on private property but are visible from a public road, street, or a place to which members of the public have access, such as the parking lot of a shop or other business establishment).

   Based on the provisions of the California Electronic Communications Privacy Act (CalECPA) - SB 178, a search warrant must be obtained after a tag is affixed to a vehicle, unless specified exceptions apply. Such exceptions include a vehicle where the occupants/operator(s) have no standing (e.g., stolen vehicle, carjacked vehicle, embezzled vehicle), a vehicle driven by a person subject to parole supervision, and a vehicle which must be located immediately to prevent death or serious physical injury. *See* Cal. Penal Code § 1546 *et seq*.

3. **Information Collected.** The StarChase system captures only the device's geographic location from the time of deployment to the time of retrieval, or until the device's battery has discharged (whichever occurs first).

4. **Safeguards.** All data will be closely safeguarded and protected by both procedural and technological means. The Palo Alto Police Department will observe the following safeguards regarding access to and use of stored data:
    a. All StarChase data shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date, and time.
    b. Persons approved to access StarChase data under this policy are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation.
    c. Such StarChase data may only be released to other authorized and verified local enforcement officials and agencies for legitimate law enforcement purposes (e.g., assistance in locating and apprehending the vehicle).
    d. Every StarChase deployment and system inquiry must be documented by either the associated case number or incident number.

5. **Retention.** The City's vendor, StarChase, will store the data (data hosting) and ensure proper maintenance and security of data stored in their data centers. StarChase will purge the data 30 days after collection, unless it has been identified as evidence in a specific criminal investigation. Additionally, the Palo Alto Police Department will retain relevant data obtained from the system if it has become, or it is reasonable to believe it will become, evidence in a specific criminal investigation or is subject to a discovery request or other lawful action to produce records. In those circumstances the applicable data should be downloaded from the server onto portable media and booked into evidence.

    Information gathered or collected, and records retained by StarChase will not be sold, accessed, or used for any purpose other than legitimate law enforcement or public safety purposes.

6. **Access by non-City Entities.** The StarChase data may be shared only with other local law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise required by law, and as provided below:
    a. Requests
        i. A law enforcement agency may make a written request for specific data, including the name of the agency and the intended official law enforcement purpose for access
        ii. The request shall be reviewed by the Chief of Police or the authorized designee and approved before access is granted
        iii. The approved request is retained on file
        iv. Requests for StarChase data by non-law enforcement or non-prosecutorial agencies will be processed by the Department's custodian of records and fulfilled only as required by law.
    b. The Chief of Police or the authorized designee will consider the California Values Act (Government Code § 7284.2 et seq.), before approving access to StarChase

data. The Palo Alto Police Department does not permit the sharing of StarChase data gathered by the City or its contractors/subcontractors for purpose of federal immigration enforcement.

7. **Compliance Procedures.** The Investigative Services Captain (or other police administrator as designated by the Police Chief) shall be responsible for ensuring compliance with procedures, including, but not limited to:
    a. Ensuring only properly trained sworn officers, crime analysts, and police staff are allowed access to the StarChase system or StarChase data.
    b. Ensuring that training requirements are completed for authorized users.
    c. Ensuring the security of the information collected and compliance with applicable laws.

    It is the responsibility of the Investigative Services Captain (or other police administrator as designated by the Police Chief) to ensure that an audit is conducted of StarChase deployment and use at least once during each calendar year. The Department will audit a sampling of the StarChase system utilization from the prior 12-month period to verify proper use in accordance with the above authorized uses. This audit shall take the form of an internal Department memorandum to the Chief of Police. The memorandum shall include any data errors found so that such errors can be corrected. After review by the Chief of Police, the memorandum and any associated documentation shall be filed and retained by the Department.