Surveillance Use Policy

Vigilant
San Diego Police Department

PURPOSE

Vigilant is an Automated License Plate Reader (ALPR) platform analytic tool. This technology is used to perform an analysis to help the investigative triangle of person, license plate, and location. It allows data returns from a variety of ALPRs from within the State of California to be reviewed by investigators.

Automated License Plate Recognition (ALPR) is a component of the San Diego Police Department's crime-fighting strategy that involves the identification of vehicles associated with suspects, witnesses, or victims. ALPR enhances the Department's ability to focus its investigative resources, deter the occurrence of crime, and enhance public safety of the community.

USE

Vigilant is used by San Diego Police Department personnel for investigative purposes.

The Vigilant database has proven to be a very effective tool in combating crime. The operation and access to Vigilant data shall be for official law enforcement purposes only.

Law enforcement purposes of Vigilant data:

- Locating stolen, wanted, or subject of investigation vehicles.
- Locating vehicles belonging to witnesses and victims of a violent crime.
- Locating vehicles associated with missing or abducted children and at-risk individuals.

Only authorized users can access the Vigilant interface. The users are primarily assigned to investigative and patrol units and have been vetted and approved by the Department's Vigilant Program Administrator as having an investigative need for the technology.

The San Diego Police Department only has access to the data Vigilant obtains from other agencies/companies that share their data with Vigilant. The Department does not collect, capture, or record any data It is an analytic tool to help investigators review data returns from a variety of ALPRs in the State of California to enhance their investigations.

The San Diego Police Department does not own any of the data nor does it provide any data to Vigilant.

Department Procedures associated with the use of the Vigilant are:

- DP 1.51- License Plate Recognition
- DP 4.13- Retention / Custody of Officer Notes, Documents, and Other Evidence.

DATA COLLECTION

The San Diego Police Department does not gather information or data. Vigilant technology is a web-based system that collects data from legally obtained sources and shares it with authorized users.

The legally obtained resources are from California law enforcement agencies and private companies (Towing Companies) which collect data using ALPR. Each individual agency or company then shares the data with Vigilant.

Surveillance Use Policy

Vigilant
San Diego Police Department

DATA ACCESS

San Diego Police Department personnel authorized to use Vigilant shall be authorized by the Chief of Police or their designee. Such personnel shall be limited to designated captains, lieutenants, sergeants, detectives, and police department personnel unless otherwise authorized.

Refer to Department Procedure 1.51 for additional information.

DATA PROTECTION

San Diego Police employees need to be granted access to Vigilant from the department administrator. Once an account is created, a 2-factor authentication is required when logging in each time. All logins, access requests to the system, and searches are tracked in an audit trail. If an authorized user has not logged on in a one-year period, the account goes inactive, and authorization is needed to reactivate the account.

Data collected by San Diego Police Department personnel through Vigilant which is downloaded to the mobile workstation or in storage shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date, and time. Only those employees of the San Diego Police Department working in an investigative or enforcement function shall access ALPR data. SDPD works with the City's Department of Information Technology, which oversees the IT governance process. For additional details related to IT governance processes, which involves risk assessment, along with data and cyber security, refer to the information at the following link:

- https://www.sandiego.gov/sites/default/files/fy23-fy27-it-strategic-plan-sd.pdf

DATA RETENTION

San Diego Police Department personnel working in an investigative or enforcement function often retain data relevant to an investigation acquired through Vigilant.

Any data retained shall follow Department Procedure 4.13- Retention / Custody of Officer Notes, Documents, and Other Evidence.

PUBLIC ACCESS

As Vigilant is a secured data analysis tool, public access is not allowed.

Data retained by San Diego Police personnel through Vigilant is included in officer / investigative reports, notes, and/or evidence.

The public can access the retained data/information by requesting a report through various means (online, mail, in-person), and or through the NextRequest Online Portal.

Surveillance Use Policy

Vigilant
San Diego Police Department

THIRD PARTY DATA SHARING

Information and/or data sets from Vigilant will not be shared with any third party except under situations authorized by law. Information shall only be shared in the following situations:

- Pursuant to a Court Order
- As part of case submission to a prosecuting agency
- As part of an ongoing criminal investigation as allowed by law
- In accordance with all applicable, state, and City laws, along with current case law.
- Per the California Public Records Act (CPRA).

TRAINING

Vigilant offers online and in-person training through the Vigilant Law Enforcement Training Academy. This training is conducted all throughout the United States several times throughout the year.

The Vigilant Program Administrator will train the user on the proper use of the Vigilant interface. All changes to the interface or other substantive changes will be handled through Vigilant with notification to the department.

All employees who utilize Vigilant technology shall be provided a copy of this Surveillance Use Policy, along with instructions of the constitutional protections and case law requirements associated with its lawful use.

AUDITING AND OVERSIGHT

Personnel who are authorized to have access to Vigilant shall ensure that their access to and use of the data complies with the Surveillance Ordinance. Vigilant and/or the Vigilant Program Administrator can provide an audit of individual users and data obtained.

Oversight will be maintained by the SPLA Unit, and auditing of ALPR technology will also be included in the Inspections Guide and added to the random inspections conducted by Research, Analysis and Planning Unit pursuant to DP 1.25.

Any misuse of this technology shall result in disciplinary actions as outlined in Department Procedure 1.51.

MAINTENANCE

The vendor maintains the security and integrity of the Vigilant system. The Vigilant technology is designed with a variety of security tools, techniques, processes, and configurations that meet or exceed the Criminal Justice Information Services Division (“CJIS”) requirements set forth by the FBI. All data transmissions and connections are made using secured connections.