Surveillance Impact Report

Vigilant

San Diego Police Department

DESCRIPTION

Vigilant is an Automated License Plate Reader (ALPR) platform analytic tool.

Vigilant technology is a web-based system that collects data from legally obtained sources and shares it with authorized users.

Vigilant is a database 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.

PURPOSE

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. Vigilant technology is a web-based system that collects data from legally obtained sources and shares it with authorized users.

Vigilant 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 identifying vehicles associated with suspects, witnesses, or victims. ALPR enhances the Department's ability to focus its investigative resources, deter crime, and enhance the community's public safety.

LOCATION

Any San Diego Police Department computer with internet access can access the Vigilant database.

City of San Diego crime statistics can be viewed at:

- Crime Statistics & Crime Mapping | Police | City of San Diego Official Website.

IMPACT

Surveillance technology's uses and deployments are not based on discriminatory or viewpoint-based factors. The Department's use of surveillance technology is intended to support and benefit the communities of San Diego while minimizing and mitigating potential impacts to community members' civil rights and civil liberties. The ALPR data collected by Vigilant does not collect personal identifying information of the driver or registered owner of the vehicle. The technology does not employ facial recognition. ALPR data collected by Vigilant are not actively monitored but are viewed in response to an alert. The information taken from Vigilant is used after the fact, only after a qualifying crime (e.g., homicide or shooting), and only when a legitimate investigative need exists. The Fourth Amendment

rights of San Diegans are not implicated because the ALPRs are physically deployed to view vehicles and license plates in public areas where the license plates and vehicles are exposed to public view. Because the cameras view data in public spaces without a reasonable expectation of privacy, no search has taken place under the Fourth Amendment. Therefore, the privacy rights of community members and visitors to San Diego will not be violated.

Refer to Department Procedure 1.51 for additional information

MITIGATIONS

The collection, use, retention, or dissemination of data shall not be used to violate the Constitutional rights of any person or in any manner that would discriminate against any person based upon their ethnicity, race, gender, natural origin, religion, sexual orientation, or gender identity.

ALPR information collected by Vigilant does not collect personal identifying information of the driver or registered owner of the vehicle. The technology does not employ facial recognition. The data taken from the Vigilant is used after the fact, only after a crime has taken place, and only when a legitimate investigative need exists. The Fourth Amendment rights of San Diegans are not implicated because the ALPRs, which Vigilant collects data from, are physically deployed to view vehicles and license plates in public areas where the license plates and vehicles are exposed to public view. Because the cameras view data in public areas where no expectation of privacy exists, no search has taken place under the Fourth Amendment. Therefore, the privacy rights of community members and visitors to San Diego will not be violated.

Refer to Department Procedure 1.51 for additional information

DATA TYPES AND SOURCES

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. The following are examples of what data Vigilant collects.

- Hotlist - A file that contains the license plate numbers of stolen vehicles; AMBER, SILVER, FEATHER, or other law enforcement alerts; lists of license plate numbers known to be associated with wanted or missing individuals. The San Diego Police Department must use a second law enforcement database to identify information for individuals associated with the license plate.
- Hotlist Sources ALPR systems - used by law enforcement; can alert on detections of wanted vehicles. Two primary methods exist for creating a wanted vehicle within an ALPR system. First, ALPR systems allow for the manual entry of both a hotplate and a hotlist. Second, the ALPR system allows agencies to import National Crime Information Center (NCIC) records as an automated hotplate source. This is the most common method for populating hotlists

- Hotplate - A license plate with a wanted status. It may also be entered into a system designed to provide a notification of future detections.

DATA SECURITY

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 and downloaded to the mobile workstation or in storage shall be accessible only through a login/password-protected system capable of documenting all information accessed 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. The San Diego Police Department 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

FISCAL COST

The Vigilant basic plan is $2500.00 a year.

The Department is forecasted to upgrade to the commercial plan at a cost of $99.995.00 annually.

THIRD PARTY DEPENDENCE

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

- 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 California State Laws.

ALTERNATIVES

Although Vigilant is not the only company providing data to law enforcement agencies, other companies at the time did not offer the same services needed by San Diego Police investigative personnel.

TRACK RECORD

Vigilant is a database proven to be a very effective tool in combating crime. Law enforcement uses the Vigilant provided data to locate stolen, wanted, or subject of investigation vehicles. Vehicles belonging to

witnesses and victims of a violent crime are discovered, along with vehicles associated with missing, abducted children, and at-risk individuals can also be found.

PUBLIC ENGAGEMENT AND COMMENTS

On November 8, 2023, at 1800 hours, there was a publicly held meeting in all nine council districts in the City of San Diego. The following surveillance technologies were presented by the San Diego Police Department:

1. Avalex DRV and FLIR-HDc
2. WHOOSTER
3. MSABs Raven Mobile Triage Tool
4. MSABs XRY Mobile Forensic Data Recovery Software
5. National ICAC Data Systems
6. PENLiNK
7. Vigilant
8. Unmanned Aircraft Systems

There were five attendees in District 1. There were zero attendees in District 2. There were zero attendees in District 3. There were zero attendees in District 4. There were zero attendees in District 5. There were zero attendees in District 6. There were two attendees in District 7. There were two attendees in District 8. There were zero attendees in District 9. There was a total of one comment and two questions out of the nine attendees. There was one comment submitted to an online public comment form.

Comment #1:

> These are all technologies that provide advanced safety to each and every citizen of our city. What I am not in favor of is the requirement that these presentations be held in nine locations throughout the City. Staffing so many locations with SDPD and San Diego Fire and Rescue personnel takes these critical First Responders away from their far more important jobs of keeping the City's citizens of San Diego safe. Our police and fire departments are already understaffed. This is a blatant misuse of our resources. Thank you.

Online Comment #1:

> The policy is vague in which instances the deployment of aerial surveillance with no safeguards to prevent misuse of this technology. Without addressing these shortcomings, I cannot support the use of DJI Avata by San Diego PD.

Question #1:

> Is the license plate reader data looking for specific cases and/or are all plates looked at to see if they fit a specific case?

Answer:

License plate readers can look for specific plates if they are involved in an active investigation. An investigator can upload license plate information into the license plate reader operating system and set an alert to notify the San Diego Police Department when the license plate is read. Investigators may upload license plate information into the license plate reader because the plate may be associated with a crime, a missing person, or an identified suspect. The SDPD Communications Division may dispatch officers to investigate a hit on a license plate reader entry. Dispatched officers will confirm that the license plate was identified by the reader correctly before any action is initiated.

Question #2:

I think it is very important that San Diego advances in technology but is also aware of some of the issues that come from having so many technologies. The questions that I have are in three phases. One has to do with lobbying from technology companies to government agencies. I sometimes have concerns over technology companies going to conferences and lobbying Fire Chiefs, Police Chiefs and many other officials during those conferences. How does the City protect itself through accountability on that?

The second is data analytics. I worked in data analytics before and one of the things that I do see is sometimes data analytics has missing information. How do we account for that through the data information that we are gathering that way we can make proper information when citizens don't report crimes that don't add up to the statistics?

The third is, what's going to happen next with all this technology?

Answer:

In terms of lobbying, there are a couple of different processes now in place. The Police Department had a process before the Privacy Advisory Board and a process that took place after. Each technology that goes forward is evaluated by Commanding Officers and personnel to see what need it fits or what mission it serves within the Police Department, Fire Department or whichever Department looks to that technology to solve a problem.

As that solution is suggested, there really is a robust process that begins with discussions throughout the various units and continues on. We look toward guidance and have an established technology process. We have significant in-house experts and a STAC Committee, Strategic Technology Alliance Committee, who look at how technology fits into the overarching goals of the City and ask questions like about their alignment. Are they repetitive in nature? How can we create efficiency and effectiveness? Then we move on and look at funding sources, purchasing and contracting, request for proposal, and what contracting needs to take place. An assessment by Risk Management and an evaluation by the City Attorney's office is done. This process is to ensure that the technology serves the Department and ultimately the City as a whole. That then goes to our City Council members for a vote, depending on the dollar amount.

Overlapping that process is our Surveillance Ordinance process. In addition to the already established process we now notify the Privacy Advisory Board, complete community outreach, and complete Use Reports and Impact Reports.

People can lobby but Commanding officers are not making any decisions based on that lobbying group due to the established process.

There is a push being made by law enforcement, and with other City departments, to use data to make informed decisions. The office of the City auditor has stressed the need for the City to use data to make more informed decisions, and that is what we are consistently striving for and implementing.

The next part of this process calls for the Police Department to hear from the community. Each one of the technologies presented has a Use Report to accompany it. After these meetings, we take the Impact Reports along with any community feedback and forward them to the Privacy Advisory Board. The Privacy Advisory Board will assess the technologies, roundtable them, form subcommittees, and make recommendations to the City Council to consider.