Surveillance Impact Report

Nighthawk LEOVision
San Diego Police Department

DESCRIPTION

Nighthawk LEOVision is a data analysis tool. This technology is used to perform a visual analysis of extensive digital data records. It allows data returns from a variety of sources (e.g., social media, search histories, cellular device data) to be synthesized, organized, and reviewed by investigators. The system only allows for analysis of information, it does not gather data sets.

PURPOSE

Nighthawk LEOVision does not gather or otherwise obtain data. It is an analytic tool to help investigators review data returns from a variety of platforms to enhance their investigations. This technology significantly reduces the amount of time that would be required to manually review these returns. This technology also allows users to synthesize multiple returns into a searchable data set to establish a timeline of activity and/or communications from a variety of data sources.

LOCATION

The Department currently has twenty (20) authorized users of the Nighthawk LEOVision tool. The users are primarily assigned to the Homicide Unit and the Crime Analysis Unit and have been vetted and approved by the Robbery Unit Lieutenant.

City of San Diego crime statistics can be viewed at Crime Statistics & Crime Mapping | Police | City of San Diego Official Website.

IMPACT

This technology does not gather information or data. This technology is a cloud-based system (Amazon GovCloud, which meets or exceeds CJIS requirements set forth by the FBI) that stores digital data record files uploaded by investigators from legally obtained sources. Legally obtained sources typically include court-approved search warrant returns and data obtained via signed consent.

This technology is a force multiplier and significantly reduces the time required to manually review large digital data returns. This technology also allows users to synthesize multiple returns into a searchable data set to establish a timeline of activity and/or communications from a variety of data sources.

The San Diego Police Department's Nighthawk LEOVision Surveillance Use Policy safeguards civil liberties and civil rights. The uses and deployments of surveillance technology are not based upon 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 on the civil rights and civil liberties of community members.

MITIGATIONS

Investigators must comply with all applicable laws, including the California Electronics Communications Privacy Act (ECPA), when requesting search warrants for data sets, including the notification requirement to users whose data is obtained.

Information and/or data sets from Nighthawk LEOVision 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 California State Laws

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

DATA TYPES AND SOURCES

This application uses social media, search histories, and cellular device data that an investigator has already collected.

DATA SECURITY

As Nighthawk LEOVision is a secured data analysis tool, public access is not allowed. All the data sets uploaded into the system will be maintained in their original form for the period allowed and/or required by law.

Access to the Nighthawk LEOVision system is restricted to those users assigned an account. The users are required to complete a multi-factor authentication process to access the technology. Users uploading data sets into the system can limit access to those having an investigative need for their case. Users without a right-to-know/need-to-know can be restricted from accessing the information, requiring approval from the uploading user to be granted access. All logins, access requests to the system, and the information uploaded and searched is tracked in an audit trail.

Nighthawk LEOVision services require that all connections use secure HTTP. Data is encrypted in transit by utilizing signed URLs for all user data transfers. User data is encrypted at rest with AES256 encryption.

FISCAL COST

The system currently costs $2,436.53 per license. The San Diego Police Department has 20 licenses. The total amount spent this year is $48,730.60. This is an annual fee and is subject to change.

THIRD PARTY DEPENDENCE

Nighthawk LEOVision is hosted in Amazon Web Services (AWS) GovCloud, a secure cloud provider compliant with FedRAMP High baseline, which meets the DOJ's Criminal Justice Information System Security Policy. The services run in a private subnet within a secure virtual private cloud.

ALTERNATIVES

There are no other known companies that provide this service

TRACK RECORD

Crime Analysis received call detail records from a suspect's phone and mapped the records in Nighthawk. The records placed the phone at the scene of several robberies. The analyst also received files from the cellphone data in a Cellebrite file and downloaded the data into the same case file in Nighthawk. The person had messages, photos and notes on their phone that showed they facilitated and participated in several robberies. By going through a variety of data simultaneously, the analyst corroborated evidence for prosecution.

PUBLIC ENGAGEMENT AND COMMENTS

On December 7, 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. Berla iVE
2. Cellebrite
3. CellHawk
4. CPClear
5. FaSTR
6. Grayshift/Graykey
7. Magnet Forensics AXIOM
8. Nighthawk
9. OffenderWatch
10. RealQuest

There were two attendees in District 1. There were two attendees in District 2. There were three attendees in District 3. There were five 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 zero attendees in District 8. There were two attendees in District 9. There was a total of one comment and five questions out of the sixteen attendees. There were no comments submitted to the online public comment form.

Comment #1:

> Comment regarding the fiscal impact and waste of City employee time for the presentations, in compliance with the ordinance.

Question #1:

> Question regarding Berla. Does it require physical access to the phone to use Berla or can you access it remotely? Does law enforcement have access to the content of messages? Does the ordinance allow clandestine access to gather data and analyze it without the owner knowing?

Answer:

Physical access to the vehicle cannot be accessed remotely. No, just date and time. No, requires physical access to the vehicle. The system typically needs to be removed from the vehicle and the process takes hours. In addition, a search warrant requires the owner to be notified.

Question #2:

Question regarding Nighthawk and social media.

Answer:

The 2016 Electronic Communications Protection Act (ECPA) search warrant requires any information gathered from social media for analysis be retained until a court order for destruction, for cross-examination, prosecution, discovery, etc.

Question #3:

Questions regarding data storage and access. Who hosts/stores the data? The city or the vendor? Where are the programs hosted/stored? Locally, statewide, federally? Which personnel gets access to the sensitive data? Is there employee access training to prevent biases?

Answer:

SDPD provides training in the handling of evidence. Evidence is downloaded and stored to retention policy dates. They can also refer to the Use Policy for further details.

Question #4:

Question regarding RealQuest. Phones connect to AppleCarPlay and AndroidAuto? Does RealQuest have access to AppleCarPlay or AndroidAuto?

Answer:

No, it is a separate system and has no access to those systems. It is devoted to real estate or real property.

Question #5:

Question regarding Nighthawk. Is Nighthawk access via a search warrant? You stated generally, but is that a requirement in this use policy?

Answer:

Access is usually through a search warrant. No knowledge of any that have been uploaded by other means. ECPA requirements are part of the review.

To maximize the reach of the materials presented at the community meetings, the Police Department created a link to the City of San Diego's technology website which provides all materials for presented technologies as well as upcoming technologies and additional materials. The materials and questions/comments section could be accessed by visiting the below web address: www.sandiego.gov/police/technology. The web address was posted in conjunction with the QR code at the community meeting.

The Department also video recorded a meeting so that it could be presented to a larger group. The benefit of the video was the capability of translating the presentation into over 100 languages such as Spanish, and other languages frequently used by the communities within San Diego, to maximize penetration of the materials to affected groups. The link to the video is at: SDPD Surveillance Technology Community Meeting 12/07/2023 (youtube.com)