Surveillance Impact Report

Magnet Forensics AXIOM
San Diego Police Department

DESCRIPTION

The Magnet Forensics AXIOM product is licensed software that can recover, process, and analyze digital evidence that has been extracted from a cell phone.

PURPOSE

The Forensic Technology Unit (FTU) utilizes the Magnet Forensics AXIOM as a data interpretation tool to analyze and categorize data extracted from cell phones.

LOCATION

The Magnet Forensics AXIOM software is located within a keycard-locked room of the Forensic Technology Unit of the Crime Laboratory located at San Diego Police Department Headquarters.

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

IMPACT

The Magnet Forensics AXIOM software does not gather information or data. This software is used on secure computer systems that are not connected to the department network or have internet access.

The San Diego Police Department's Magnet Forensics AXIOM 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

Only members of FTU have access to this software and are required to have a unique login and password. Access to FTU is restricted by keycard access and requires a dongle to use the software.

DATA TYPES AND SOURCES

Magnet AXIOM software does not gather information or data. It recovers and analyzes digital evidence from mobile devices, computers and cloud services.

DATA SECURITY

Only Criminalists in the FTU who have completed training and have been authorized by the laboratory Quality Manager to perform extractions may use the Magnet AXIOM software.

There is no public access to the data analyzed by the Magnet AXIOM software. If a criminal defendant wishes to obtain the interpreted data from the Magnet AXIOM software related to their case, it must be obtained through a court order or the discovery process.

FISCAL COST

The annual cost of the software license is approximately $8,671.

THIRD PARTY DEPENDENCE

Magnet reports can only be obtained by San Diego Police Department investigators or the District Attorney via a search warrant or the court process in accordance with California State Law. There is no third-party sharing.

ALTERNATIVES

There are no known alternatives, as this is proprietary software.

TRACK RECORD

Magnet Forensics AXIOM is a software tool used by every law enforcement agency in the United States including the FBI and the Internet Crimes Against Children taskforce. It has been in use in the department for more than 7 years. Since almost every person has a cell phone, it is crucial to helping solve crime. It is a clearly established software for law enforcement and the crime laboratory, and it has been used thousands of times. It has been used to help victims of domestic violence as well as children who have been abused. It has been used to solve numerous homicides as well as human trafficking cases.

There are no known adverse actions related to the use of this software. There are no cases of violations associated with this software. There are no known controversies. It is a very common software for creating reports of extracted cell phone data. After a thorough search, there were no unanticipated costs, operational failures, or issues related to civil rights or liberties related to this software. The department and crime laboratory follows the California Electronic Communication Privacy Act to safeguard the information contained on a person’s cell phone. The law is broader than the federal law.

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)