Surveillance Impact Report

Grayshift GrayKey
San Diego Police Department

DESCRIPTION

Grayshift GrayKey is a hardware and software tool used by the Forensic Technology Unit to extract cell phone data without altering the data or adding data to the phone.

PURPOSE

When proper authority, such as a search warrant or consent form, is obtained, cell phones are connected to the Grayshift GrayKey tool, and the data is extracted from the phone. Grayshift GrayKey is designed to complete the extraction without altering any of the data or adding data to the phone.

LOCATION

The Grayshift GrayKey tool is located within a keycard-locked room of the Forensic Technology Unit (FTU) of the Crime Laboratory located at San Diego Police Department Headquarters. The extracted data is stored on the SDPD's Network Attached Storage (NAS) in Data Systems. Only investigators with a search warrant can access the data controlled by Data Systems.

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

IMPACT

This tool is only used with proper legal authority to search a cell phone or consent from the owner of the phone. The data extracted using Grayshift GrayKey technology is only used in criminal investigations and is not available to the public.

The San Diego Police Department's Grayshift GrayKey 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 authorized users (criminalists) in the Forensic Technology Unit (FTU) who have completed training and have been authorized by the Quality Manager to perform extractions may use the Grayshift GrayKey tool. Copies of the data can only be obtained with a court order or through the discovery process.

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.

DATA TYPES AND SOURCES

Due to the large variety of cell phone models and manufacturers, not all cell phones can be extracted through Grayshift GrayKey. Only phones that are supported by the vendor can have data extracted.

Surveillance Impact Report

Grayshift GrayKey
San Diego Police Department

Grayshift GrayKey can extract call logs, text messages, emails, photos, videos, contacts, browsing history, app data, and location data. Grayshift GrayKey can also extract data from some social media applications on a phone.

Grayshift GrayKey software can also analyze deleted data and hidden files on a device and can recover data that has been deleted.

DATA SECURITY

Grayshift GrayKey software and equipment are stored and maintained in the FTU, a secured office within SDPD Headquarters. Only authorized users have access to the technology. Each user is required to use a unique login and password to access the software and conduct data extractions.

The Grayshift GrayKey software is not located on Department network computers and can only be accessed by logging into a computer inside SDPD Headquarters containing the installed software. The computer used with the software has no internet access and is not accessible by the vendor. Additionally, the software can only be installed through a specific process and cannot be moved, and the user must be authorized with a valid software license. The Grayshift GrayKey software cannot be accessed outside of SDPD Headquarters.

FISCAL COST

Grayshift GrayKey software and equipment were initially purchased for $15,000. The license is renewed yearly at approximately $27,995, funded through the IT Budget.

THIRD PARTY DEPENDENCE

Data extracted using Grayshift GrayKey technology is not shared without a court order or other legal proceedings, such as discovery. The extracted data is considered confidential, and there is no third-party access or sharing. Grayshift GrayKey does not have access to the extracted data.

ALTERNATIVES

There are other tools, such as Cellebrite Universal Forensics Extraction Devices, that the SDPD also uses at a higher cost, however, Cellebrite does not extract cell phones in the same way. Grayshift GrayKey's proprietary software can extract phones that would otherwise be locked.

TRACK RECORD

Grayshift GrayKey is a hardware and 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 tool 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 that 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 tool. There are no cases of violations associated with this tool. There are no known controversies. It is a very common tool for cell phone

extraction. There are no unanticipated costs, operational failures, or issues related to civil rights or liberties related to this tool. The Department and the Crime Laboratory follow 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. In addition to this, the vendor has rules for the use of its product and requires the Department to sign a contract that the tool will be used in accordance with certain guidelines.

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)