Surveillance Use Policy

Grayshift GrayKey
San Diego Police Department

PURPOSE

The GrayKey tool 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.

USE

When proper legal authority, as defined by the California Electronic Communications Privacy Act [ECPA; SB 178 (2016) codified in Penal Code 1546.1], is obtained, cell phones are connected to the GrayKey tool, and the data is extracted from the phone. GrayKey is designed to complete the extraction without altering any of the data or adding data to the phone. There is no way to limit what data is extracted using the GrayKey tool.

Due to the large variety of cell phone models and manufacturers, not all cell phones can be extracted. Only phones that the vendor supports can have data extracted.

DATA COLLECTION

GrayKey is capable of extracting call logs, text messages, emails, photos, videos, contacts, browsing history, app data, location data, and more. GrayKey can also extract data from many social media apps, such as Facebook Messenger, Instagram, and Snapchat, on the phone. The applications that can be extracted depend on a number of factors, including the device's make, model, operating system, and security updates.

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

The extracted data is then stored on the department's Network Attached Storage (NAS) in Data Systems. Only investigators with a search warrant can access the data controlled by Data Systems.

DATA ACCESS

Only authorized users (criminalists) in the Forensic Technology Unit (FTU) that have completed training and have been authorized by the Quality Manager to perform extractions may use the GrayKey tool (see Training below for more details). Extracted data is accessible only by the FTU and the requesting investigator. Extracted data is stored on SDPD networks which are managed by the FTU and IT/Data Systems analysts. The resulting report(s) generated from extracted data are only reviewed when proper legal authority has been obtained to review those report(s).

DATA PROTECTION

The GrayKey software and equipment are stored and maintained in the FTU, a secured office within Police 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 GrayKey software is not located on department network computers and can only be accessed by logging into a computer with the software installed inside the building. The computer ~~has no internet access and~~ is not accessible by the vendor. Additionally, the software can only be installed through a

specific process. It cannot be moved, and the user must be an authorized user with a valid software license. The GrayKey software cannot be accessed outside of the Department.

DATA RETENTION

Other than homicides and violent sexual assaults, where extracted data is kept indefinitely, extracted data is retained based on the statute of limitations for the associated crime or if the case has been adjudicated. Data is purged from the NAS when it is at the end of its retention period.

PUBLIC ACCESS

The data extracted using GrayKey technology is only used in criminal investigations and is not available to the public. Copies of the data can only be obtained with a court order or the discovery process.

THIRD PARTY DATA SHARING

Data that has been extracted using-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. The vendor does not have access to the extracted data.

TRAINING

FTU criminalists must successfully complete an in-house extensive training program comprised of: literature review; lectures; practical exercises; shadowing; passing a written test, practical tests, and moot court; and completing supervised casework. The training program, which is outlined in the FTU manual, complies with the American National Standards Institute (ANSI) National Accreditation Board's (ANAB) International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 17025 Forensic Testing Laboratory standards. To satisfy the on-going requirements of ANAB accreditation, FTU criminalists are also required to pass annual proficiency tests for each technology utilized.

AUDITING AND OVERSIGHT

As an ANAB-accredited forensic testing laboratory, FTU is extensively audited annually to ensure that all policies and procedures are followed, and in accordance with the standards set by ANAB. One portion of this is specifically dedicated to auditing a random sampling of each FTU criminalist's usage of the tools. Prior to its initial usage in casework, the tool's capabilities and limitations were assessed in a comprehensive validation study. It was approved for casework by the FTU Technical Lead and Crime Laboratory Quality Assurance (QA) Manager. All updates to the software are verified prior to use in casework by FTU analysts. FTU criminalists also must annually pass a proficiency exam utilizing the GrayKey tool. All qualification records are maintained by the Crime Laboratory's QA Manager.

The Crime Lab's Administrative Support Unit and the FTU supervisor (or designee) ensure that legal authority to search each device is valid. The FTU supervisor authorizes the use of the tools each time a device is assigned to an FTU criminalist for extraction/analysis. The performance of each tool is monitored by each FTU criminalist, and oversight of the performance of all tools is maintained by the

FTU Technical Lead. Every tool usage by an FTU criminalist is audited by another FTU criminalist and the FTU supervisor (or designee).

SDPD's Research and Planning Unit audits equipment utilized by FTU annually.

The GrayKey tool physically resides in the SDPD Crime Laboratory's Forensic Technology Unit. Key card access is required to enter the FTU. Key card access logs are audited annually.

IT/Data Systems maintains oversight over computer access. IT/Data Systems monitors logins to the GrayKey computer for unauthorized access on a daily basis. Only FTU criminalists have authorized log-ins to the GrayKey computer.

Data is only extracted with proper legal authority. Department policies, State of California laws, and laboratory policies outline how extracted data is maintained. Misuse of the system, data, or resulting reports must be reported to and investigated by the Department. Violations of laws, Departments Policies, or user agreement terms would subject the department member to discipline and / or criminal proceedings or civil processes.

MAINTENANCE

The GrayKey tool is controlled and maintained by the vendor and FTU, following laboratory quality policies and department policies. FTU criminalists are responsible for monitoring and updating software when new versions are released. A log documenting all software updates is maintained by the FTU.