Surveillance Use Policy

MSAB's Raven – Mobile Triage Tool
San Diego Police Department

PURPOSE

MSAB's RAVEN – Mobile Triage Tool is a device and software used to extract cell phone data by members of the Internet Crimes Against Children Task Force (ICAC) while in the field.

RAVEN is a handheld device taken into the field by investigators and is used to preview data contained on smartphones and tablets. Only trained task force members have access to the tool. The device is kept secure in the ICAC task force office. Additionally, the device requires a unique login to access the tools. That login is made available only to trained ICAC investigators.

Once the data is extracted, Odin, part of the RAVEN software, is used to categorize extracted data into easy-to-view, searchable, and filtered files for assigned investigators.

USE

When proper authority, such as a search warrant or consent, is obtained, smartphones and/or tablets are connected to the RAVEN tool, and the data is extracted from the phone. RAVEN is designed to complete the extraction without altering any of the data or adding data to the phone. The data can then be previewed on-scene, allowing the investigator to determine the evidentiary value of the device.

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

DATA COLLECTION

RAVEN can extract call logs, text messages, emails, photos, videos, contacts, browsing history, app data, and location data.

Raven can extract SIM card information to include, user identity, location, phone number, network authorization data, personal security keys, contact lists, and stored images and text messages.

Raven also can extract information from thumb drives, SD cards, and Micro SD cards, allowing investigators the ability to quickly analyze the contained data.

As the tool is used to triage, assisting investigators on the scene of search warrant services to determine the evidentiary value of the device being analyzed, only data extracted from confirmed evidence is retained. That extracted data is downloaded and stored on the task force's Network Attached Storage (NAS) located in the secured ICAC office. All data extracted from devices determined not to be of evidentiary value is deleted.

DATA ACCESS

Only task force members, investigators, and certified forensic examiners, who have been trained and certificated by MSAB and have been authorized by the task force commander to perform on-scene triage extractions may use the RAVEN mobile triage tool.

All new users must receive training from MSAB before being given access to the system.

Surveillance Use Policy

MSAB's Raven – Mobile Triage Tool
San Diego Police Department

DATA PROTECTION

The RAVEN mobile triage tool is stored and maintained in ICAC, in a secured office located away from San Diego Police Headquarters. Only authorized users have access to the office space and technology.

The RAVEN mobile triage tool is not located on a department network computer and can only be accessed by logging in to the device itself. The device has no internet access and is not accessible by the vendor. Additionally, Raven is downloaded onto a mobile device by the vendor, it cannot be moved or altered, and the user must be an authorized user with a valid software license. The RAVEN triage tool cannot be accessed by anyone other than the authorized user.

DATA RETENTION

Per evidence code sections related to crimes perpetrated against children allowing for historical evidence to be brought forth, extracted data is retained until the death of the suspect.

PUBLIC ACCESS

The data extracted using RAVEN 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 through the discovery process.

THIRD-PARTY DATA SHARING

Data that has been extracted using RAVEN 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. MSAB does not have access to the extracted data.

TRAINING

Investigators and certified forensic examiners who use the RAVEN software must complete and pass a training program provided by MSAB before using the software.

AUDITING AND OVERSIGHT

ICAC maintains a log of all authorized RAVEN users. ICAC is also responsible for all RAVEN software updates and granting access to the system.

Data is only extracted via legal authority, such as a search warrant or consent. Misuse of the system would be reported to and investigated by the task force member's Internal Affairs unit. Violations of the laws, agency policies, or user agreement terms and conditions would subject the task force member to discipline and/or criminal proceedings or civil processes.

MAINTENANCE

The RAVEN software is controlled and maintained by the vendor and ICAC. The ICAC commander is responsible for monitoring and updating software when new versions are released.