Surveillance Impact Report

MSAB's XRY – Mobile Forensics and Data Recovery Software
San Diego Police Department

DESCRIPTION

MSAB's XRY software is used to extract cell phone data by members of the Internet Crimes Against Children task force (ICAC). XRY can extract call logs, text messages, emails, photos, videos, contacts, browsing history, app data, and location data. XRY can also extract data from some social media apps on the phone. This information is utilized in the investigation into child exploitation and/or enticement cases.

Once the data has been extracted, MSAB's XAMN, part of the XRY software, is used to categorize extracted data into readable reports for assigned investigators.

XRY--as described on MSAB's website (https://www.msab.com/product/xry-extract/):

> "XRY is a powerful, intuitive and efficient mobile data recovery software that runs on the Windows operating system. It lets you securely extract more high-quality data in less time than ever before, while always completely maintaining the integrity of the evidence."

PURPOSE

ICAC task force members utilize the XRY software to access and extract data contained within smartphones and/or tablets relevant to an investigation. That data, information such as call logs, text messages, emails, photos, videos, contacts, browsing history, app data, and location data, is then analyzed to determine its evidentiary value and to develop investigative leads. This type of data is used in active investigations into the sexual exploitation and/or enticement of children.

LOCATION

XRY is maintained on a computer, not linked to City or Department networks, located at the San Diego ICAC's secure law enforcement office. Only authorized members of the task force have access to the office.

City of San Diego crime statistics can be viewed at:

- Crime Statistics & Crime Mapping | Police | City of San Diego Official Website.

IMPACT

Data extracted and analyzed by XRY is obtained only with proper legal authority, such as approved search warrants or with written consent of the possessor of the device. Only authorized task force members who have successfully passed training provided by MSAB may utilize this tool.

SDPD's XRY Surveillance Use Policy safeguards civil liberties and civil rights. Surveillance technology's uses and deployments are not based on 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 community members' civil rights and civil liberties.

MITIGATIONS

Data retained is limited to the files extracted by the software and selected by the task force member to be downloaded into their digital case file located on the ICAC Network Attached Storage (NAS) system located in the secured ICAC office. XRY does not retain data.

This data is obtained via proper legal process or with the consent of the possessor of the device. Extracted files are organized by case and housed in a folder specifically created for that case on the ICAC NAS.

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.

The general public has no access to the XRY system or information contained in the ICAC NAS database.

DATA TYPES AND SOURCES

XRY can extract call logs, text messages, emails, photos, videos, contacts, browsing history, app data, and location data from smartphones, tablets, and loose storage media. XRY can also extract data from some social media apps on smartphones and tablets. This type of data is used in active investigations into the sexual exploitation and/or enticement of children.

DATA SECURITY

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 extractions may use XRY software.

All new users must receive training from MSAB before being given access to the system. Only trained investigators are authorized to use XRY to conduct an extraction. XRY software and equipment are stored and maintained in ICAC, a secured office located away from San Diego Police Headquarters. Only authorized users have access to the office space and technology.

The XRY software is not located on a department network computer and can only be accessed by logging in to the computer with the software installed. 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 XRY software cannot be accessed outside of the task force.

FISCAL COST

Grant funds awarded to the ICAC task force through the Office of Juvenile Justice and Delinquency Program/DOJ are used to fund this tool. XRY's cost to the task force is approximately $6,000 per fiscal year. It is a recurring cost factored into ICAC's annual budget.

There are no ongoing or personnel costs associated with it.

THIRD-PARTY DEPENDENCE

No extracted data is retained or accessible by MSAB.

Data that has been extracted using XRY 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.

ALTERNATIVES

ICAC has used XRY since 2015. Additionally, ICAC uses two other forensics tools to conduct smartphone/tablet extractions and analysis. Each tool has proprietary differences and capabilities. As a result, each tool extracts data differently and obtains slightly different data. To ensure ICAC investigators locate and extract the best possible evidence for their cases, ICAC uses all three industry-leading tools, including XRY. ICAC has a long-standing, excellent working relationship with MSAB's personnel, which has benefited our users many times over.

TRACK RECORD

XRY is used primarily by law enforcement agencies but also by prisons/correctional institutions, intelligence agencies, tax authorities, border control agencies, the military, and selected private companies. MSAB remains one of the leaders in their respective industry, and as such, extractions, analyses, and reports created from their software tools have been successfully presented and testified to in court cases an untold number of times nationally and internationally.

An example of its use is when ICAC conducted an undercover proactive investigation where an investigator, posing as a child, was contacted by an individual determined to be a sex registrant on parole. During chat communication with the suspect, he arranged to meet the decoy, a thirteen-year-old child, for sex. Ultimately, the suspect was arrested and his devices were forensically examined. During that examination, XRY successfully extracted all of the chats the suspect had with the decoy, corroborating the communication, as well as multiple images of child sexual assault material. The suspect was charged and pleaded to multiple charges, resulting in a seven-year prison sentence.

PUBLIC ENGAGEMENT AND COMMENTS

On November 8, 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. Avalex DRV and FLIR-HDc
2. WHOOSTER
3. MSABs Raven Mobile Triage Tool
4. MSABs XRY Mobile Forensic Data Recovery Software
5. National ICAC Data Systems
6. PENLiNK

7. Vigilant
8. Unmanned Aircraft Systems

There were five attendees in District 1. There were zero attendees in District 2. There were zero attendees in District 3. There were zero 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 two attendees in District 8. There were zero attendees in District 9. There was a total of one comment and two questions out of the nine attendees. There was one comment submitted to an online public comment form.

Comment #1:

> These are all technologies that provide advanced safety to each and every citizen of our city. What I am not in favor of is the requirement that these presentations be held in nine locations throughout the City. Staffing so many locations with SDPD and San Diego Fire and Rescue personnel takes these critical First Responders away from their far more important jobs of keeping the City's citizens of San Diego safe. Our police and fire departments are already understaffed. This is a blatant misuse of our resources. Thank you.

Online Comment #1:

> The policy is vague in which instances the deployment of aerial surveillance with no safeguards to prevent misuse of this technology. Without addressing these shortcomings, I cannot support the use of DJI Avata by San Diego PD.

Question #1:

> Is the license plate reader data looking for specific cases and/or are all plates looked at to see if they fit a specific case?

Answer:

> License plate readers can look for specific plates if they are involved in an active investigation. An investigator can upload license plate information into the license plate reader operating system and set an alert to notify the San Diego Police Department when the license plate is read. Investigators may upload license plate information into the license plate reader because the plate may be associated with a crime, a missing person, or an identified suspect. The SDPD Communications Division may dispatch officers to investigate a hit on a license plate reader entry. Dispatched officers will confirm that the license plate was identified by the reader correctly before any action is initiated.

Question #2:

> I think it is very important that San Diego advances in technology but is also aware of some of the issues that come from having so many technologies. The questions that I have are in three phases. One has to do with lobbying from technology companies to government agencies. I sometimes have concerns over technology companies going to conferences and lobbying Fire

Chiefs, Police Chiefs and many other officials during those conferences. How does the City protect itself through accountability on that?

The second is data analytics. I worked in data analytics before and one of the things that I do see is sometimes data analytics has missing information. How do we account for that through the data information that we are gathering that way we can make proper information when citizens don't report crimes that don't add up to the statistics?

The third is, what's going to happen next with all this technology?

Answer:

In terms of lobbying, there are a couple of different processes now in place. The Police Department had a process before the Privacy Advisory Board and a process that took place after. Each technology that goes forward is evaluated by Commanding Officers and personnel to see what need it fits or what mission it serves within the Police Department, Fire Department or whichever Department looks to that technology to solve a problem.

As that solution is suggested, there really is a robust process that begins with discussions throughout the various units and continues on. We look toward guidance and have an established technology process. We have significant in-house experts and a STAC Committee, Strategic Technology Alliance Committee, who look at how technology fits into the overarching goals of the City and ask questions like about their alignment. Are they repetitive in nature? How can we create efficiency and effectiveness? Then we move on and look at funding sources, purchasing and contracting, request for proposal, and what contracting needs to take place. An assessment

by Risk Management and an evaluation by the City Attorney's office is done. This process is to ensure that the technology serves the Department and ultimately the City as a whole. That then goes to our City Council members for a vote, depending on the dollar amount.

Overlapping that process is our Surveillance Ordinance process. In addition to the already established process we now notify the Privacy Advisory Board, complete community outreach, and complete Use Reports and Impact Reports.

People can lobby but Commanding officers are not making any decisions based on that lobbying group due to the established process.

There is a push being made by law enforcement, and with other City departments, to use data to make informed decisions. The office of the City auditor has stressed the need for the City to use data to make more informed decisions, and that is what we are consistently striving for and implementing.

The next part of this process calls for the Police Department to hear from the community. Each one of the technologies presented has a Use Report to accompany it. After these meetings, we take the Impact Reports along with any community feedback and forward them to the Privacy Advisory Board. The Privacy Advisory Board will assess the technologies, roundtable them, form subcommittees, and make recommendations to the City Council to consider.