No images? Click here

Optimizing Computer & Internet Monitoring

by Brian J. Kelly, Director - Spotlight Division

Brian Kelly was the first U.S. Probation Officer to officially hold the title of Cybercrime Specialist in the federal Judiciary. Appointed to the position in October 2000, Brian formulated the Eastern District of New York Probation Office Cybercrime policies and procedures, which included the creation of the district's Computer & Internet Management/Monitoring Program. Brian was also a member of the national Cybercrime Working Group (AOUSC), tasked with formulating national policy and training in the area of Cybercrime for the federal Judiciary.

Computer and Internet management/monitoring in community corrections involves a multifaceted approach encompassing a range of strategies and considerations to effectively supervise and

manage computer and Internet usage of persons under supervision (PUS). This includes clear and specific guidelines for PUS, along with configuring devices and monitoring software appropriately, with the goal of ensuring maximum data capture for visibility, and effective relevant flagging.

There are three key steps for optimizing computer and Internet management/monitoring.

1. **Instructions/Restrictions:** Establishing clearly defined parameters for PUS while being monitored sets guardrails and expectations for all stakeholders while removing the possibility of plausible deniability. One strategy is to create an agency Computer & Internet Acceptable Use Contract that can be executed at the start of monitoring. The parameters should allow for customization based on special needs like education and employment, as well as unique risk factors.
2. **Device Configuration:** Preparing a device for monitoring has several steps. An important component is conducting a pre-installation analysis of the device to ensure a clean starting point. Depending on jurisdiction, this can require additional legal authorizations. Analysis should include assessment of device hardware and identifications (e.g. serial numbers), installed software, and user content. Traditional digital forensics requires specialized training and equipment, and can be time consuming. “Live” analysis tools can streamline this process, but examiners must be properly

trained and aware of potential evidentiary concerns (see my June 2022 article "Compliance Analysis" which includes information on IPPC Technologies' Express Scan). Device configuration can also involve uninstalling unnecessary or potentially harmful programs, apps, and files based on the instructions/restrictions.

3. **Monitoring Configuration:** Configuration of monitoring parameters include establishing profile and baseline settings based on the scope, risks, and needs. This includes the addition and removal of keywords to flag the most relevant information. It is also important for agencies and officers to make ongoing adjustment and modifications of settings based on observed user behavior, emerging threats, and changing requirements.

Regular review and analysis of collected data to identify patterns, anomalies, and potential risks is the culmination of all three steps.

Additional considerations for comprehensive computer and Internet monitoring include managing third-party apps and their potential for circumventing monitoring measures. Staffing models and resource allocation should be evaluated to ensure adequate supervision and support. Ongoing training for staff and individuals involved in the monitoring process is essential to stay informed about emerging technologies, online risks, and best practices in computer and internet monitoring.

Officers can improve the relevance of information received from Spotlight by entering the following

information in the Case Details section of each case in the Next Gen interface:

- Offense: arrest/conviction and prior criminal conduct
- Preference: age, gender, details
- Contact with Minors Restriction (YES/NO)
- Organization Affiliation
- Current Areas of Concern

Officers can access and edit Case Details by logging into the IPPC NextGen interface and clicking on the appropriate Case Number.

If a custom RISK word is added to case settings in Next Gen, such as a victim name, officers can add tags to identify those custom RISK words for the Spotlight team. After adding the custom word, click Add Tag and several checkboxes will appear for selection. The current options are:

- Victim
- Officer
- Co-Defendant
- Treatment Provider

Multiple tags can be selected. Please be sure to save settings before exiting.

IPPC Technologies continues to strive towards predictive and proactive solutions so officers can intervene early, address areas of concern and change behavior. Spotlight is a data analysis service provided by IPPC Technologies that uses human verification augmented with artificial intelligence (AI) technologies to validate content captured and flagged by IPPC's monitoring and analysis solutions. Spotlight's mission is to provide agencies and officers with streamlined and

verified leads, for possible intervention opportunities related to concerning behaviors. For more information on Spotlight, please call IPPC at (888)-WEB-IPPC or contact me directly at bkelly@ippctech.net or by calling (516)341-4201.

Agencies receiving the Spotlight service can give feedback any time via the Spotlight Performance Survey: https://forms.office.com/r/K9JpsNjKH

IPPC TECHNOLOGIES
PO BOX 60144
KING OF PRUSSIA, PA 19406
TEL: 888-WEB-IPPC (932-4772)
INFO@IPPCTECH.NET
WWW.IPPCTECH.NET