Computer, Cellphone, & Mobile Device Extraction Tools

Seattle Police Department (SPD)

What is the technology?

Computer, cellphone, and mobile device extraction tools are used to pull private information from the devices of individuals. The different extraction tools SPD utilizes for mobile devices work similarly to one another – a mobile device is physically connected to a computer workstation with specialized locally installed software or to a stand-alone device with a similar software installed. The software is able to bypass/decipher/disable the device's PIN/password and extract files containing data from the mobile device.

Why do we use the technology?

SPD utilizes electronic device extraction and imaging technologies to recover digital information or data from computers, cell phones, and mobile devices as part of a criminal investigation. These technologies are utilized only with the device owner's consent or pursuant to search warrant authority. Extraction tools allow investigators to legally collect evidentiary information for ongoing investigations that may be used to prosecute crimes. These tools allow investigators to extract data quickly and securely from a wide variety of devices and preserve evidence from these devices in forensically sound conditions which can then be presented in court.

The open comment period for this technology is currently underway. You can provide comments to **Seattle.gov/SurveillanceComment**.

All comments will be included in the Surveillance Impact Report on this technology and submitted to Council.

If you would like to provide feedback outside of the open comment period, please submit them directly to City Council.

Collection

Data extraction devices are utilized only after legal standards of consent or court-issued warrant have been met. Extraction tools for mobile devices, excluding computer imaging, collect information from electronic devices, including contact lists, call logs, Short Messaging Service (SMS) and Multi-Media Messaging Service (MMS) messages, and GPS locations. Computer imaging collects an entire image of a computer's hard drive at a specific point in time. Data collected from the extractions is provided to the requesting Officer/Detective for inclusion in the investigation file and is stored following evidence guidelines.

Use

Extraction tools are maintained in two units within SPD: Sexual Assault and Child Abuse (SAU) Unit and the Technical and Electronic Support Unit (TESU). Investigators complete a request form which includes a copy of the consent or search warrant authorizing the extraction. The Unit Supervisor will screen all tracking technology deployments to ensure that the appropriate authorities are in place before approving deployment of tracking technology.

Equipment deployment is constrained to the conditions stipulated by the consent or court order providing the legal authority.

Protections

All device utilization is documented and subject to audit by the Office of Inspector General and the federal monitor at any time. All information must be gathered and recorded in a manner that is consistent with SPD Policy 6.060, such that it does not reasonably infringe upon "individual rights, liberties, and freedoms secured by the Constitution of the United States and of the State of Washington, including, among others, the freedom of speech, press, association and assembly; liberty of conscience; the exercise of religion; and the right to petition government for redress of grievances; or violate an individual's right to privacy."

City of Seattle