SURVEILLANCE TECHNOLOGY IMPACT REPORT

Department or Division:	Somerville Police Department (SPD)
Compliance Officer (name and position):	Lt. Sean Sheehan
Submitted by:	Lt. Sean Sheehan
Date:	10/10/2023
Surveillance Technology:	GrayKey

X	**Please identify the purpose(s) of the proposed surveillance technology. Select ALL that apply by entering "X" in the left column.**
X	Identifying and preventing threats to persons and property and preventing injury to persons or significant damage to property
X	Identifying, apprehending, and prosecuting criminal offenders
X	Gathering evidence of violations of any law in criminal, civil, and administrative proceedings
X	Providing information to emergency personnel
	Documenting and improving performance of City employees
	Executing financial transactions between the City and any individual engaged in a financial transaction with the City
	Preventing waste, fraud, and abuse of City resources
	Maintaining the safety and security of City employees, students, customers, and City-owned or controlled buildings and property
	Enforcing obligations to the City
	Operating vehicles for City business
	Analyzing and managing service delivery
	Communicating among City employees, with citizens, or with third parties
	Surveying and gathering feedback from constituents
	Other (Describe): If the surveillance technology is used for a purpose not listed above, does the purpose comply with the surveillance use policy? ___ Yes ___ No

Complete ALL of the following items related to the proposed surveillance technology. Be as specific as possible. If an item is not applicable, enter "N/A." Do NOT leave fields blank.

1. Information describing the surveillance technology and how it works:

The GrayKey Digital Forensics Analysis Tool (DFAT) is used to legally access digital evidence located on electronic devices which include, but are not limited to, Computers, Mobile Phones, Digital Cameras, Tablets and any device used to communicate, store data and facilitate the commission of crimes. A valid search warrant issued by the appropriate jurisdictional Massachusetts Court, or a valid consent to search is required in order to legally extract the evidence from the device. Through the Urban Area Security Initiative (UASI) Boston Office the SPD has acquired a License for the GrayKey Digital Forensics Analysis Tool and a Laptop computer which is used to analyze the data extracted from these devices.

a. Authorized use – the uses that are authorized, the rules and processes required before that use, and the uses that are prohibited (10.64.b.2):

A valid search warrant, issued by the appropriate jurisdictional Massachusetts Court, or a valid consent to search is required in order to legally extract the evidence from the device.

Similar to the search of a car or a home, search of a phone is subject to limitations laid out in case law, and the scope and terms of the warrant. The technology cannot be used to collect personal information unrelated to the investigation. The information gathered must be relevant to the investigation as indicated in the search warrant.

b. Training – the training, if any, required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology, including whether there are training materials (10.64.b.9):

One Detective and one Detective Supervisor will be trained on the use of the GrayKey DFAT.

2. Information on the proposed purpose(s) for the surveillance technology (10.64.b.1):

The technology would only be used in cases in which a search warrant has been obtained in conjunction with the investigation allowing access to the device in question or with the owner's consent. Devices that contain digital evidence must be properly collected, handled and processed. The volatile nature of the data on these devices requires proper seizure to preserve the integrity of the data and ensure their evidentiary value in legal proceedings. Devices must be processed properly, whether the data these devices contain are incriminating or exculpatory.

3. Information describing the kind of surveillance the surveillance technology is going to conduct and what surveillance data is going to be gathered (10.64.b.3):

This technology opens "locked" devices by overriding passcodes. The types of surveillance data obtained from these devices include photos, videos, text conversations, call logs and any data normally stored on an electronic device.

a. Data access – the individuals who can access or use the collected surveillance data, and the rules and processes required before access or use of the information (10.64.b.4):

The GrayKey Hardware, including the Laptop computer used to analyze the data, will be housed in a secure room(Digital Forensics room) with access limited to three individuals in the SPD, the two GrayKey trained detectives, and their supervisor, the Criminal Investigation Division(CID) Commander. Access to the room will be limited by key card access and hard copy key to these three individual officers. In addition, the Digital Forensics room is located in an area of the SPD where access is limited to authorized individuals with key card authority.

The GrayKey extraction tool work terminal is password protected. A password is also required to access the actual GrayKey tool itself before an extraction is attempted. The user license for the tool has a specific serial number associated with it, which identifies the licensed unit that performs an extraction. In addition, SPD utilizes write-blocking software that is also password protected which prohibits copying of any files from the terminal.

b. Data protection – the safeguards that protect information from unauthorized access, including, but not limited to, encryption, access-control, and access-oversight mechanisms; (10.64.b.5)

The device is used by two detectives, one of which is a supervisor, who are both certified by GrayKey. These two detectives will be under the direct supervision of the CID Commander. Information retrieved is stored on one specific computer, under the direct control of the Digital Forensics Detective.

c. Data retention – the time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason that retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period has elapsed, and the conditions that must be met to retain information beyond that period (10.64.b.6):

Any data or evidence obtained from using this technology would be retained for the duration of the relevant investigation and pending legal proceedings.

d. Public access – if and how collected surveillance data can be accessed by members of the public, including criminal defendants (10.64.b.7):

Data collected is not available to members of the public. Defendants can request the data through the criminal discovery process.

e. Third-party data-sharing – if and how other city or non-city entities can access or use the surveillance data, including any required justification and legal standard necessary to do so, and any obligation(s) imposed on the recipient of the surveillance data (10.64.b.8):

Data may be shared with the District Attorney's Office and/or other Law Enforcement Agencies if the investigation is multi-jurisdictional.

4. The location(s) it may be deployed and when:

The technology will only be deployed when a valid search warrant is issued by the courts or if valid signed consent is presented. Detectives are required to seek their supervisor's approval prior to using the technology.

5. A description of the privacy and anonymity rights affected and a mitigation plan describing how the department's use of the equipment will be regulated to protect privacy, anonymity, and limit the risk of potential abuse:
The device would be used by a single trained member of the department, under the authorization of a supervisor, and only with consent or a search warrant.
6. The potential impact(s) on privacy in the city; the potential impact on the civil rights and liberties of any individuals, communities or groups, including, but not limited to, communities of color or other marginalized communities in the city, and a description of whether there is a plan to address the impact(s):
This device is used specifically in conjunction with a criminal investigation. Authority to use this technology would be granted by a valid search warrant or consent and could not be used indiscriminately.
7. An estimate of the fiscal costs for the surveillance technology, including initial purchase, personnel and other ongoing costs, and any current or potential sources of funding:
There is no cost for the device as all License costs are paid for by UASI Boston.
8. An explanation of how the surveillance use policy will apply to this surveillance technology and, if it is not applicable, a technology-specific surveillance use policy:
The City's Surveillance Use Policy will apply.
a. Oversight – the mechanisms to ensure that the surveillance use policy is followed, including, but not limited to, identifying personnel assigned to ensure compliance with the policy, internal record keeping of the use of the technology or access to information collected by the surveillance technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the sanctions for violations of the policy (10.64.b.10):
There are two Detectives, one a supervisor, trained and authorized to use the technology. Any misuse of this device would lead to department discipline up to and including termination.