APPENDIX A: SURVEILLANCE TECHNOLOGY IMPACT REPORT

Department or Division:	Somerville Police Department (SPD)
Compliance Officer (name and position):	Lt. Jeff DiGregorio
Submitted by:	Lt. Jeff DiGregorio
Date:	
Surveillance Technology:	GreyKey

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
	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 Somerville Police Department does not possess this technology, but have used it in the past with the cooperation of other agencies) This technology opens locked devices (computers and cell phones) by bypassing any passcodes to gain access to the device.
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):
This device would be used under the authorization of a 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 is trained in using this device.
2. Information on the proposed purpose(s) for the surveillance technology (10.64.b.1):
This device 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.
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.
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):
Only the investigator and investigator's supervisor would have access to the data recovered.
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)

This device is used by one member of the detective bureau and under the direction of a supervisor and under the authorization of a search warrant.

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):

This would not apply as the device unlocks computers and phones and does not collect data.

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

There would be no data collected but access to electronic devices. Thus there would be no public access to information obtained. Criminal defendants could request information through discovery rules.

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):

This technology would be used specifically to named investigations and under the authority of a search warrant. There would be no third party sharing unless the investigation involved another law enforcement agency or the crimes investigation were multi-jurisdictional.

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

This device would only be deployed in investigations under authority of supervisor's approval and search warrant.

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 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 would be used specifically, in conjunction with an active criminal investigation. Any authority to use

this device would be granted by a search warrant, 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 as this device is not owned by the city nor the police department

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:

Since this device can look at data in locked devices the city's policy would 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 is only one investigator trained and authorized to use this device. Its use is first authorized by a detective supervisor, and also by the laws of the Commonwealth. Any misuse of this device would lead to department discipline up to and including termination.